

SECURE SYSTEM FOR ACTIVATING PERSONAL COMPUTER SOFTWARE AT REMOTE LOCATIONS

Patent number: JP6501120T

Publication date: 1994-01-27

Inventor:

Applicant:

Classification:

- **International:** G06F13/00; G06F15/00; H04L9/00; H04L9/00; H04L9/10; H04L9/12

- **European:** G06F1/00N7R2; G06F9/445; G06F9/445N; G06F21/00N7P5M

Application number: JP19910501845T 19911106

Priority number(s): US19900610037 19901107; US19910682456 19910409

Also published as:

WO9209160 (A1)
EP0556305 (A1)
US5222134 (A1)
EP0556305 (A4)
EP0556305 (B1)

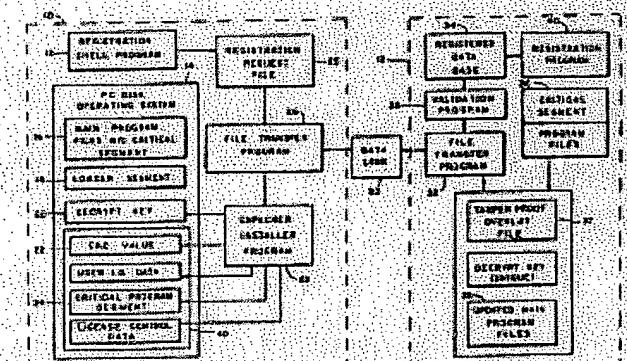
[more >>](#)

[Report a data error here](#)

Abstract not available for JP6501120T

Abstract of corresponding document: **US5222134**

A process and system for activating various programs are provided in a personal computer. The computer is initially provided with a registration shell. A data link is established between the personal computer and a registration computer. By providing the registration computer with various information, a potential licensee can register to utilize the program. Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer and transferred to the personal computer. The tamperproof overlay includes critical portions of the main program, without which the main program would not operate and also contains licensee identification and license control data.



Data supplied from the **esp@cenet** database - Worldwide

BEST AVAILABLE COPY

(19)日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表平6-501120

(43)公表日 平成6年(1994)2月3日

第6部門第3区分

(51) Int.Cl.¹ F I
 G 0 6 F 13/00 3 5 1 H 7368-5B
 15/00 3 3 0 A 7459-5L
 H 0 4 L 9/00
 9/10

7117-5K H 0 4 L 9/ 00 Z
 審査請求 有 予備審査請求 有 (全 8 頁) 最終頁に続く

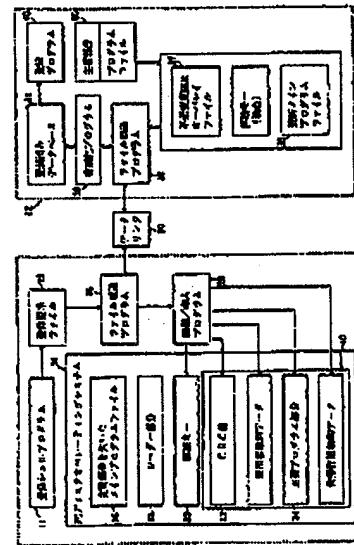
(21) 出願番号 特願平4-501845
 (26) (22) 出願日 平成3年(1991)11月6日
 (25) 翻訳文提出日 平成5年(1993)5月7日
 (26) 国際出願番号 PCT/US91/08069
 (27) 國際公開番号 WO92/09160
 (27) 國際公開日 平成4年(1992)5月29日
 (31) 優先権主張番号 610,037
 (32) 優先日 1990年11月7日
 (33) 優先権主張国 米国(US)
 (31) 優先権主張番号 682,456
 (32) 優先日 1991年4月9日
 (33) 優先権主張国 米国(US)

(71) 出願人 タウ・システム コーポレイション
 アメリカ合衆国 バージニア州 フォルス
 ティアード、リースバーグ バイク,
 7115, スーツ327
 (72) 発明者 ワイト、デービット、ビー
 アメリカ合衆国 バージニア州 22032,
 フェアファックス ギルバートソン ロー
 ド, 4220
 (72) 発明者 リッセル、ホライス、ジー
 アメリカ合衆国 バージニア州 22021,
 チャンチリイ、パレイ カウントリ ドラ
 イブ, 13811
 (74) 代理人 弁理士 倉持 晴 (外1名)
 最終頁に続く

(54)【発明の名称】 パーソナルコンピュータのソフトウェアを遠隔位置で起動するための安全システム

(57)【要約】

様々なプログラムを起動するための過程とシステムがパーソナルコンピュータ(10)に提供されている。パーソナルコンピュータ(10)には、登録シェルプログラム(11)が当初備わっている。データリンク(30)がパーソナルコンピュータ(10)と登録用コンピュータ(12)の間に確立される。登録用コンピュータ(12)に様々な情報を与えることにより、見込み被許諾者はメインプログラム(16)の使用を登録することができる。ひとたび登録過程が完了すると、不正変更防止オーバーレイプログラムが登録用コンピュータ(12)において作成され、パーソナルコンピュータ(10)に転送される。不正変更防止オーバーレイには、メインプログラム(16)の主要部分がよくされ、これを欠くとメインプログラム(16)は動作せず、また不正変更防止オーバーレイには使用許諾箇別データと使用許諾割合データも含まれている。



特許平6-501120 (2)

時号化オーバーレイファイル内にあるとともに、解説キーを上記オーバーレイファイルに接する請求の範囲第1項に記載の方法。

6. 上記オーバーレイが実行のためにロードされるたびに巡回冗長検査値が計算され、上記不正変更防止オーバーレイファイル内に伝送された巡回冗長検査値と比較され、上記オーバーレイファイルが正常以降変更されているかどうかを判断することを特徴とする請求の範囲第1項に記載の方法。

7. 上記使用者識別情報を上記オーバーレイファイルとが、電子データクリッピングを介して上記変換シェルと上記登録プログラムとの間を伝送されることを特徴とする請求の範囲第1項に記載の方法。

8. 上記登録シェルプログラムが、上記の独立した登録用コンピュータを備えた第二の遠隔コンピュータから離れた、第一のコンピュータ内に接続されることを特徴とする請求の範囲第1項に記載の方法。

9. 上記使用者識別と上記オーバーレイファイルが、一台のコンピュータに入力され得ることを特徴とする請求の範囲第1項に記載の方法。

10. プログラムファイルを削除されたもしくは削除されない間隔導入などのシステムにおいて、
オーバーレイローダー部分が含まれているが少なくとも一つの

- 【請求の範囲】
1. プログラムファイルを組合する方法であって、
表示装置を有する遠隔コンピュータに対して、ローダーセグメントと登録シェル部分を含むプログラムファイルを提供し、上記プログラムファイルは主要部分を欠いてい、上記プログラムファイルを正しく実行することを能止する工程。
使用者識別情報を上記登録シェル部分に入力する工程。
上記使用者識別情報を、上記登録シェルから登録用コンピュータ内にある独立した登録プログラムに送達し、上記登録プログラムは使用者識別データと上記主要部分とを符合して各自のオーバーレイファイルを生成する工程。
上記の各自のオーバーレイファイルを上記登録プログラムから上記登録シェルに伝送する工程、上記オーバーレイファイルには上記プログラムファイルには当初欠けている主要部分が含まれ、そして
上記オーバーレイファイルを上記メインプログラムファイルに導入する工程を有し、上記オーバーレイファイルに入っている使用者識別が導入されたときだけ上記プログラムファイルの動作を可能とすることを特徴とする前記のプログラムファイル起動方法。
 2. 上記オーバーレイファイルを上記登録用コンピュータから上記遠隔コンピュータに伝送する前に、上記使用者識別情報を判別可能にする工程を有する請求の範囲第1項に記載の方法。
 3. 不正変更防止のオーバーレイファイルを作成する工程を有する請求の範囲第1項に記載の方法。
 4. 上記不正変更防止オーバーレイファイルが上記オーバーレイファイルを暗号化することにより作成され、巡回冗長検査値が上記

主要プログラム部分が欠けているプログラムファイルが当初備わっていて、このプログラムファイルが動作することを防止し、上記オーバーレイローダー部分は本部のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを実行することができ、上記遠隔コンピュータには登録シェルプログラムが備えられ、上記登録シェルプログラムは使用者が様々な使用者識別情報を入力することを可能にするような少なくとも一の遠隔コンピュータと。

登録プログラムと、上記使用者識別情報を受信し処理するための手段と、上記プログラムファイルに欠けている上記主要プログラム部分と使用者識別情報の全部あるいは一部を含む各自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに寄付する手段。

上記オーバーレイファイルを上記遠隔コンピュータに伝送することで、上記オーバーレイファイルに入っている使用者識別が現在導入されているときだけ上記プログラムファイルの動作が可能になることを特徴とする上記プログラムファイル起動システム。

11. 上記遠隔コンピュータと上記登録用コンピュータとの間を結合する電子データクリッピングと、上記登録用コンピュータと上記遠隔コンピュータの両方に備えられているファイル転送手段とを含むことを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

12. 上記登録用コンピュータが、すべての登録済み使用者が含まれている中央ゲートベースと上記使用者識別情報を複数化するための手段とを有していることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

13. オーバーレイファイルを作成するための上記手段が、巡回冗長検査値を備える不正変更防止オーバーレイファイルを作成するための巡回冗長検査値と解説キーを備えており、上記解説キーは上記オーバーレイファイルと共に上記遠隔コンピュータに伝送されることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

14. 上記遠隔コンピュータが、上記オーバーレイファイルを解説し、上記オーバーレイファイルが実行のためにロードされるたびに巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータによって上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

15. 上記主要部分がエクゼクティブ部部分であり、そして上記使用者識別情報を使用許認証情報であることを特徴とする請求の範囲第1項に記載の方法。

16. 上記主要プログラム部分がエクゼクティブ部部分であり、そして上記使用者識別情報を使用許認証情報であることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

17. 上記主要エクゼクティブ部部分がプログラムファイル全体を有することを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

18. プログラムファイルの使用を制御する方法において、
表示装置を有するコンピュータに対してローダー部分と登録シェル部分を含むプログラムファイルを提供し、上記プログラムフ

答表平6-501120(9)

ファイルは第一レベルの制御機能を有するエグゼクティブ制御プログラムを有しております。

情報を上記登録シエル部分に入力し、

上記使用許諾契約情報を上記登録シエルから当社登録プログラムに伝送し、上記登録プログラムは使用許諾契約データを第二レベルの制御機能を有するエグゼクティブ制御プログラムに併合して独自のオーバーレイファイルを発生し、

上記独自のオーバーレイファイルは上記登録プログラムから上記登録シエルに伝送し、上記オーバーレイファイルには上記第二レベルのエグゼクティブ制御プログラムが含まれており、そして上記独自オーバーレイファイルを上記主要プログラムファイルに導入し、上記プログラムファイルの第二レベルの機能の動作が上記オーバーレイファイル内の使用許諾契約情報が読み込まれていもとだけ可能になることを特徴とする上記のプログラムファイル使用の処理方法。

19. 上記オーバーレイファイルは上記登録用コンピュータから上述機コンピュータに伝送する以前に、上記使用許諾契約情報を有効化する工程を有する際の範囲第18項に記載の方法。

20. 不正変更防止になっているオーバーレイファイルを構成する工数を有する請求の範囲第18項に記載の方法。

21. 上記不正変更防止オーバーレイファイルが上記不正変更防止オーバーレイファイルを暗号化キーで暗号化することにより作成され、巡回冗長検査値を上記暗号化不正変更防止オーバーレイファイル内に提供するとともに解密キーを上記不正変更防止オーバーレイファイルに発行し、上記暗号化および解密キーは上記オーバーレイファイルの独自の内容によって暗号に決定されることを特徴とする請求の範囲第20項に記載の方法。

上記登録シエルプログラムは使用者が様々に使用許諾契約情報を入力することを可能にするよう少なくとも一台の遠隔コンピュータと、

登録プログラムと、上記使用許諾契約情報を受信し処理するための手段と、第二レベルの機能を有するプログラムモジュールと使用許諾契約情報の全般あるいは一部を含む各自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記遠隔コンピュータに伝送することで、上記オーバーレイファイルに入っている使用許諾契約情報が現在使われているときだけ、上記プログラムファイルの第二レベルの機能動作が可能なることを特徴とする上記システム。

22. 上記遠隔コンピュータと上記登録用コンピュータとの間に電子データリンクを有し、ファイル転送過程が上記登録用コンピュータと上記遠隔コンピュータの双方に備えられていることを特徴とする請求の範囲第27項に記載のシステム。

23. 上記登録用コンピュータが、すべての登録済み使用者が含まれる中央データベースと上記使用許諾契約情報を有効化する手段とを備えていることを特徴とする請求の範囲第27項に記載のシステム。

24. オーバーレイファイルを作成するための上記手段が、巡回冗長検査値が記憶されている不正変更防止オーバーレイファイル作成するための暗号化キーと解密キーとを備えており、上記解密キーは上記オーバーレイファイルと共に上記遠隔コンピュータには送り、上記暗号化および解密キーはファイルの内容によって独自に決定されることを特徴とする請求の範囲第27項に記載のシステム。

25. 新しい巡回冗長検査値が、上記オーバーレイが実行のためにロードされるたびに計算されて、上記オーバーレイファイルと共に送された巡回冗長検査値と比較され、上記オーバーレイファイルが作成直後変更されているかどうかを判断することを特徴とする請求の範囲第21項に記載の方法。

26. 上記使用許諾契約情報を上記オーバーレイファイルが、上記登録シエルと上記登録プログラムとの間を電子データリンクを介して伝送されることを特徴とした請求の範囲第18項に記載の方法。

27. 上記登録シエルプログラムが、上記登録用プログラムを備えた第二のコンピュータから離れている第一のコンピュータに備えられていることを特徴とする請求の範囲第19項に記載の方法。

28. 上記有効化により上記使用許諾契約情報を正真的登録シエルを介して確保することを特徴とする請求の範囲第10項に記載の方法。

29. 上記使用許諾契約情報を上記オーバーレイファイルが一台のコンピュータに記載され、備えられることを特徴とする請求の範囲第18項に記載の方法。

30. 制限されたあるいは制限されない期間、プログラムファイルとアップグレードするシステムにおいて、

第一レベルの機能を有するプログラムを含むオーバーレイローダー部分を含むプログラムファイルが書き換わって、上記オーバーレイローダー部分は本物のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記遠隔コンピュータには登録シエルプログラムが用いられる。

31. 上記遠隔コンピュータが、上記オーバーレイファイルを解説し、上記オーバーレイファイルが実行のためのロードされるたびに新しい巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータにより上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第30項に記載のシステム。

特許平6-501120(4)

【明細書】
パソコンコンピュータのソフトウェアを基盤並置で起動するための安全システム

発明の範囲

一般的に、パソコンコンピュータあるいはそれに類似した装置の使用者の大部分は、それら並置で実行するソフトウェアを様々な小売店からあるいは基盤並置を経て入手する。いずれの場合も、ソフトウェア製品はいわゆる「収納包装」材で包装されており、その収納包装材を破った時点でのソフトウェア製品に対する使用可否契約が成立して、その製品の使用許諾者を該使用許諾者/購入者による朱記可接觸あるいは使用から強制するようになっている。この方法による商法は、許諾者と被許諾者の双方にとって満足すべきものではないことが分かれている。たとえば、被許諾者にとっては、ソフトウェアプログラムを操作させてみてからそれが被許諾者が必要としているものかどうかを判断する場合が多えられない。さらに、非禁錮の側面からみると、この方法では被許諾者の難易ができないこと、許諾者によるプログラム使用の制御あるいは監視を行なうことができない。

ソフトウェアアプリケーション方式は、Thomsonの米国特許第4,446,519号に概要表示されており、プログラミングされた「はい/いいえ」で答える問題がプログラムに組み込まれており、そのソフトウェアが使用許可されるコンピュータに保護されているハードウェアあるいはファームウェア保護装置の存在を確認するようになっている。この技術の弊害は、プログラムが操作的保護装置をしでは使用できないようにすることであり、これはソフトウェアよりも複雑なことがはるかに困難である。しかし、このような技術は、正しい信号化店舗が見れられ、そしてそれをわずかに変更してプログラムに書き込まれてしまえば、簡単に打ち破られてしまう。ひとたび打ち破られると、通常の追跡コピーが作成され配布される可能性がある。

本発明の目的は、動作可能プログラムは、購入者/被許諾者と販売者/許諾者との間の相互の契約において入手可能になる。販売者と購入者との間は、本発明の目的に照しては、許諾者/被許諾者が契約の策定である必要はないが、以下では販売者を被許諾者、購入者を被許諾者としくは使用者と呼ぶ。ひとたび被許諾者が特定の契約条件に合意すると、被許諾者は契約データを登録用コンピュータに与えられる。登録用コンピュータはその販売者を記録し、使用可されたプログラムの可動部分を提供する。これらの部分は不正変更防止が施されていると同時に、販売された被許諾者にとって独自のものとなっている。この情報の交換に基づき、販売コンピュータプログラムが登録済み被許諾者のコンピュータに不正変更防止ファイルに吸収されて記録される。同時に、このファイルには被許諾者独自の情報を含まれている。本発明の実施例としては様々なもののが考えられるが、いずれの実施例も被許諾者を識別する独自のデータと保護されているソフトウェアプログラムに関する情報とが含まれている暗号化パッケージの構造を持っていて、したがって、被許諾者は認証ではなく、そして保護されたソフトウェアは使用許諾契約に違反できる情報を防ぐことができる。さらに、使用許可契約データを暗号化パッケージに含めることにより、様々な制限を設けて使用許可契約の条件を遵守させることができる。

一般的に、様々な実施例は、ソフトウェアのデモンストレーション版を有する可能性のあるマーケティングシェルプログラムの最初の起動が伴う。このシェルプログラムは、兎本表示と宣伝記述だけを有しているか、あるいは完全なプログラムの動作不能版を有している。しかし、大部分の実施例は、登録プログラムと、ローテーザグメントと呼ばれる特別のプログラムモジュールを含むような構成になっている。

マーケティングシェルは通りな方法で自由に販売されるであろう。マーケティングシェルがプログラムのデモンストレーション

Millenの米国特許第4,746,830号は、中央（遠隔）コンピュータを使用して、正しい信号の入手を試みる悪意のプログラムがアクセスできないマスタークリストあるいはアルゴリズムから得られたコット所除コードあるいは有効化コードを提供することを暗示している。しかし、この方法は、仮想守のコードを侵入することにより、あるいは基盤の周囲をプログラミングすることにより、もしくはデバッガープログラムによりプログラムを分割してプログラムの実行を可能にするコードの存在を見つけ出すことにより、簡単に見破られてしまう。ひとたびこの保護が打ち破られると、動作可能なプログラムの複数個のコピーが作成され記憶される可能性がある。

さるに、Schaidtの米国特許第4,849,510号に暗示されている方法では、最も優秀のあるアルゴリズムを無効化し、無効化されたプログラムを実地実験で実行すると同時に、回復アルゴリズムを別の物理的に分散し保護された処理装置で実行することにより回復し、有効機能を2つの処理器の相互連絡によって強制するようになっている。このような方法は、回復アルゴリズムの物理的保護に依存しており、この物理的保護が侵入された場合、悪意のプログラムによって簡単に打ち破られる可能性がある。したがって、そのような方法は、回復記憶媒体の物理的保護が無効できない大量市場においては、実用的ではない。

そのため、ソフトウェアを乗務員専用から保護しつつソフトウェアを大量市場に配布するための技術的な方法が求められる。さらに、見る人購入者/被許諾者がソフトウェア製品を購入者に試してみることができるような方法とシステムも必要である。また、ソフトウェア製品の改良および更新部分を登録専用者に配布するための方策も必要である。

発明の図式と範囲

本発明は、パソコンコンピュータのソフトウェアプログラムあるいは他の種類のプログラムを、使用許可を管理した方法で配

布する方法とシステムに関する。動作可能プログラムは、購入者/被許諾者と販売者/許諾者との間の相互の契約において入手可能になる。販売者と購入者との間は、本発明の目的に照しては、許諾者/被許諾者が契約の策定である必要はないが、以下では販売者を被許諾者、購入者を被許諾者としくは使用者と呼ぶ。ひとたび被許諾者が特定の契約条件に合意すると、被許諾者は契約データを登録用コンピュータに与えられる。登録用コンピュータはその販売者を記録し、使用可されたプログラムの可動部分を提供する。これらの部分は不正変更防止が施されていると同時に、販売された被許諾者にとって独自のものとなっている。この情報の交換に基づき、販売コンピュータプログラムが登録済み被許諾者のコンピュータに不正変更防止ファイルに吸収されて記録される。同時に、このファイルには被許諾者独自の情報を含まれている。本発明の実施例としては様々なもののが考えられるが、いずれの実施例も被許諾者を識別する独自のデータと保護されているソフトウェアプログラムに関する情報とが含まれている暗号化パッケージの構造を持っている。したがって、被許諾者は認証ではなく、そして保護されたソフトウェアは使用許諾契約に違反できる情報を防ぐことができる。

したがって、使用者がプログラムを実行する毎に、ローテセグメントが提供された暗証キーを使用して、暗号化ファイルを保護されていないファイルに対するオーバーレイとしてロードして解説する。このプログラムは保護されていないソフトウェアプログラムの設計にしながら実行され、独自の使用許諾データもプログラム実行中にロードされる。プログラムが実行されていないときは、保護されているプログラムはその暗号化部屋に留まって、保護されていないプログラムファイルと共にコンピュータの大容量記憶装置に保持されている。保護されているプログラムは実行のためにロードされたときだけ解説され、正しい暗号化キーにアクセスしなければ実行され得ない。

図式的範囲と範囲

図1は本発明による登録過程を示す流れ図である。

図2は本発明によるプログラム実行過程を示す流れ図である。

図3は、本発明の図式による代償的なパソコンコンピュータと登録用コンピュータの構造図である。

図4は、本発明の知見による代償的なパソコンコンピュータと登録用コンピュータに付する実施例を示す構造図である。

特許平6-501120(5)

発明の詳細な説明

本発明の目的は、許諾者がそのプログラムの費用対効果に関する情報を従来使用されている方法よりもはるかに効率的な方法で提供することを可能にすることである。さらに、本発明の第二の目的は、被許諾があるいは使用者が特定のプログラムの購入あるいは使用許諾を得るために試用することを可能にすることである。さらに、本発明の更なる目的は、特定のプログラムの使用許諾権がされたアップグレード権を登録許諾者に配布する手段を提供することである。したがって、発明の如きは包括的なものと考えられ、そしてどのようなソフトウェアプログラムも本方法によつて配布できるものと想図されている。

一実施例において、動作可能なエグゼクティブ複数ループを除いて完全な新規プログラムが、パーソナルコンピュータあるいは他の装置において、仕様ディスク、ファームウェア、ハードウェアあるいは他の手段で最初に提供される。さらに、この特定プログラムには登録シェルプログラムも含まれる。ただし、小さいプログラムもしくは複数のあるプログラムの場合、プログラム自身は存在せず、シェルだけが提供される。ニザグクティア複数ループが除外されているため、このプログラムは正しい登録権を実現しなければ動作しない。図1および図3に示されているように、この登録過程は、パーソナルコンピュータ(PC)10内部の登録シェルプログラム11と登録用コンピュータ12内部に提供されている登録プログラム40とを使用して開始される。登録システムプログラムが登録用コンピュータ12内に提供され、電子データリンク30を介して登録シェルプログラムがアクセスできる。この電子データリンクは、ローカルエリアネットワークでもよく、電話をテミングでもよく、あるいはその他のいかなる接続であつてもよい。ただし、第二の実施例においては、登録シェルおよび登録システムプログラムは同一の媒体上に存在してもよいが、その媒体は製品専用プログラムとは別でなければならない。この場

合、登録シェルおよび登録システムプログラムが入っている存取媒体の媒体は、許諾された導入プログラムによって使用者パーソナルコンピュータ10へ個人的に移植され、電子データリンクは必要ではない。

登録シェルプログラムは、使用者がTCGオペレーティングシステム14のメインプログラム内に提供されている製品専用プログラムの各行を最初に実行すると実行される。登録シェルは、製品専用プログラムに関する記述情報を提供しそれをPC表示装置に表示すると同時に、見込み被許諾者を経て信頼者として登録する。使用許諾は、特定の使用場所における権利の被許諾者に対して授与され、その期間は極々最もしくは一時的でよく、そのための費用は被許諾者に対して課せられない。ただし、登録シェルは、不正変更防止オーバーレイファイルが存在しないかぎり、メインプログラムを実行しない。登録シェルプログラム11は、登録用のPCに表示されてもデータ入力形式を提供し、被許諾者に対して、請求書番号、日付番号、使用許諾条件などの識別情報の提供を要求する。この情報は、被許諾者が再確認する登録用ファイル25に入力される。そして、登録シェルプログラムは、被許諾者が暗号キーを押して登録を開始するを得つ。このキーが押されると、登録ファイルが清じ、そして登録シェルファイル伝送プログラム26が登録システムファイル伝送プログラムとのデータリンクを確立する。登録用コンピュータ内の登録プログラム10は、データリンクが正常な登録シェルで確定されていることを確認する後密接接続チェックを行つて有効化手段42によって保護される。つまに、登録シェルは登録要求ファイル35を、そのファイルを発信する登録システムに送信し、必要なリードエフェクトと、結合されたファイル伝送プログラム26および32間のハンドシーケンス動作を実行する。完全な登録要求ファイルが中央登録用コンピュータで受けられると、登録要求が登録済み使用者34のデータベースに記入して格納される。操作には、その要求に答えるべきかど

うかを判断する様々なチャックが含まれる。たとえば、一時的使用料に対する要求が特定の被許諾者から得度送られてきた場合、その被許諾名には使用許可が含まれず、そしてそのプログラムのニザグクティア複数ループは通過されない。そのような状態が発生した場合、選択可能なメッセージが登録シェルに表示され、見込み被許諾者に対して表示される。しかし、要求が確定されると、登録済み使用者データベースへの記録が作成されるが、この過程全体が完了するまで、そのデータベースには入力されない。

登録用コンピュータ12の内部では、つまに使用登録キーが使用されて、使用登録キーとエグゼクティブ複数ループプログラムを介して合30とを結合することにより作成された暗号の不正変更防止オーバーレイファイルが生成される。結合されたデータとプログラムファイルは各自で、不正変更防止オーバーレイファイル15内に含まれる巡回冗長検査(CRC)値が計算される。一式の暗号の暗号化キーと解暗号キーが作成され、不正変更防止オーバーレイファイルの内容全体が暗号化キーを使用して暗号化される。この暗号化キーに基づき、不正変更防止オーバーレイファイルと共に暗号化される解暗号キーが提供される。暗号化アルゴリズムは、登録用暗号化システムのように、暗号化と解密にそれぞれ異なるキーを使用する仕組であればなんでもよい。登録システムが、不正変更防止オーバーレイファイルと解暗号キー、パーソナルコンピュータ登録シェルは伝送される1個の圧縮ファイル38に組み込む。また、更新されたメインプログラムファイルもこの圧縮ファイルに組み込まれ、ファイル伝送プログラムとすでに確立されているデータリンクを通じてPCの登録システムに伝送される。

当該ファイル一式の発送と同時に、登録シェルプログラム内の開閉一導入プログラム16が圧縮ファイルを開き、エグゼクティブ複数ループセグメント36、CRC値22ならびに暗号キー30および、含まれている場合は、更新メインプログラムファイルを含む不正変更防止オーバーレイファイル40を導入する。これで登録過程が

完了したので、電子データリンクを切断する。登録データベースレコードが入力され、そして被許諾者の要求に対する結果が、中央登録用コンピュータ12における別のプログラムによって実行される。

登録が終了すると、被許諾者のパーソナルコンピュータに導入された秘密暗号製品専用プログラムを起動して、不正変更防止オーバーレイファイルと解暗号キーを使用して製品専用プログラムを実行するたびに実行する製品専用プログラムをロードするためのプロセスが開始される。

このプログラム実行過程を図2に示す。表示されているように、パーソナルコンピュータの使用者が製品専用プログラムの実行をオペレーティングシステムに命令すると、オペレーティングシステムはメインプログラムとロードセグメントをロードする。ロードセグメントは他のすべてのプログラム命令に先立って実行される。つまに、ロードセグメントは製品専用プログラムの起動を実行し、不正変更防止オーバーレイの存在をチェックする。不正変更防止オーバーレイ導入されていないければ、ロードセグメントは終了してオペレーティングシステムに戻るので、メインプログラムファイルの実行が事前に防止される。不正変更防止オーバーレイが導入されていれば、ロードセグメントは解暗号キーを見つけて不正変更防止オーバーレイの解暗号とロードを行ない、メインプログラムファイルに対して存在しないエグゼクティブ複数ループプログラム命令ならびに暗号化された暗号化キーを読み出せる。解暗号およびロード過程において巡回冗長検査が実行され、それが完了すると、不正変更防止オーバーレイが登録用コンピュータからパーソナルコンピュータに伝送されたときに作成された不正変更防止オーバーレイに記憶された巡回冗長検査値と比較される。巡回冗長検査が一致になると、そのオーバーレイは固有の方法によって変更が加えられたものとなるときれ、したがって無効とされる。この時点で、ロードセグメ

特表平6-501120 (5)

シトはそのオーバーレイを取り外し、終了してオペレーティングシステムに戻る。したがって、不正変更防止オーバーレイが含まれていない場合と同様に、メインプログラムファイルの実行は、不正変更防止オーバーレイとの部分が置き換えられていても、事前に防ぐことができる。巡回冗長検査の結果、オーバーレイが置き換えられていないことが確認されると、ローダーセグメントはオーバーレイを含むメインプログラムファイルの実行を開始し、そして製品専用プログラムが最後まで実行される。

不正変更防止オーバーレイを動作可能な形態の製品専用プログラムに含めることを要求することにより、技術者と巡回冗長検査アーケードそれは以前動作可能なプログラムに常に含まれられることになる。このようにして、技術者は不正使用を防止するとともに監視することができる。

想定：および図を参照しながら説明したように、本発明によると、登録過程によって、メインプログラムファイルのニゲゼタディアブリューループセグメントと使用許可制御データとを含む不正変更防止オーバーレイファイルが生成される。登録過程が完了すると、この不正変更防止オーバーレイは登録用コンピュータからペソナルコンピュータに転送される。この不正変更防止オーバーレイは、起動後には不正使用を防止するキー装置である。なぜなら、ニゲゼタディアブリューループプログラムを介して、専用なしに各自の使用許可制御データと使用許可制御データから分離することもできなければ、該当部署別と使用許可制御データも完全な形には復元できないからである。

この不正変更防止オーバーレイファイルは、オーバーレイファイルが生成されるときに最初に巡回冗長検査をオーバーレイファイルに記憶させるとで不正変更防止になるとみなされる。巡回冗長検査は、プログラム命令と使用許可制御データを含むオーバーレイファイルの内部全体に対して対応される。該当部署データは該当であるので、各々のCPCは独自なものになる。記憶されてい

るCRC値が、オーバーレイがロードされたたびにローダーセグメントによって計算された巡回冗長検査値と比較される。これらの巡回冗長検査値が一致しなければ、ローダーセグメントは終了してオペレーティングシステムに戻る。したがって、オーバーレイファイルの内容になんらかの変更が加えられていれば、記憶されている巡回冗長検査値に対応する変更が行われないかぎり、そのオーバーレイファイルは無効になる。つまに、不正変更防止オーバーレイの内部全体が、巡回冗長検査値の位置が不明になるような方法で暗号化されるので、この種の戻をつきとめてそれを実現することが困難になる。

また、暗号化により、不正変更防止オーバーレイに含まれる特定のプログラム命令ならびに独自の使用許可制御データと使用許可制御アーケードがはっきりしなくなる。暗号化は、公開暗号化システムのように暗号化と解読に別々のキーを使用する状態によって達成される。暗号化ならびに各自の暗号化キーおよび解読キー発生のためのアルゴリズムは登録システム内に搭載し、したがって技術者はアクセスが不可能である。解読キーは、登録システムと登録プログラムシェルを通じて該当部署のコンピュータに伝送される。オーバーレイファイルを暗号化するためのアルゴリズムはローダーセグメント内にあるので、解読キーと解読アルゴリズムを使用してオーバーレイファイルを解読しその内容を検査することは、困難ではあるが可能である。しかし、内容を検査して新しい変更されたオーバーレイファイルを暗号化する読み込みは、暗号化キーに対するアクセスができるために防止される。私的暗号化キーで暗号化されたオーバーレイファイルだけしかあらかじめ解読解読キーで解読できず、私的キーは公共キーから容易には得られないという。公的暗号システムの一特徴である。

不正変更防止オーバーレイファイルは、プログラム命令のエグゼクティブブリューループセグメントと、使用許可制御データと制御部署の使用許可制御データとを有している。このデータには、

初期状態の削除、コンピュータの製造番号、コンピュータのモデルの電話番号、そしてその他の情報を含まれる。

ローダーセグメント18は若狭目的のサブプログラムであり、これは、ローダー用プログラムが取り除かれたり巡回された場合、メインプログラムファイルを動作不能にする仕組によって製品専用プログラムのメインプログラムファイルに結合される。この場合は、特定のプログラム命令と製品専用プログラムのメインプログラムファイル内部に内蔵するアルゴリズムである。これらの内部命令とは、使用者にとっては既知の記憶位置は異なる場合の組合せを検査する。ローダープログラムセグメントは、その他の属性の間にこの動作を実行する。したがって、ローダーセグメントを取り外したり巡回したりすると、メインプログラムファイルには肯定の位置における特定の組が含まれないことになり、そのため動作不能になる。

別の実施例において、登録シエルは、製品専用プログラムの動作可能なデモンストレーション版を含んでいる可能性があるマーケティングパッケージの一環として配布される。デモンストレーション版のプログラムは、ローダーセグメント、デモンストレーション版の解説キー、そしてデモンストレーション版の不正変更防止オーバーレイを含むように設計されている。この場合、不正変更防止オーバーレイには独自の使用許可制御データは含まれないが、実体性の製品の機能と表示のデモンストレーションだけを行なうメインプログラムエグゼクティブブリューループが含まれるであろう。デモンストレーション版のニゲゼタディアブリューループは、エグゼクティブブリューループの必要設計によって得られたプログラムの複数の複数を有している。たとえば、起動時を提供するケモンストレーションメニューをプログラミングして選択肢を表示することができるが、デモンストレーション版のエグゼクティブ

ブリューループをプログラミングして選択項目を製品登録情報として表示して、製品を動作させる前に登録することを可能である。

登録を開始する前に、見込み登録者はプログラムを実行し、デモンストレーション版が実行されであろう。前述したように、デモンストレーション版の解説キーが使用され、デモンストレーション版のニゲゼタディアブリューロード、解説、そして実行される。デモンストレーション版が終了すると、見込み登録者は、登録者として登録し登録版のプロダクションを実行するための一時的使用許可を得るように指示される。そして、使用者は前述のようにして登録を行い、図4に示されているプロセスを開始することができる。登録要求に応答して、新しいオーバーレイファイル40'を独自の暗号キー-20'が含まれている自身のファイルが登録用コンピュータから送られる。巡回プログラムファイルと実行版のプログラムファイルも、自身のファイルと共に受け取られる。登録プログラムはデモンストレーション版の不正変更防止オーバーレイ40と解説キー-20をそれぞれの整体版40'と共に置換する。

登録後も、使用者がプログラムを実行すると、プログラム実行過程で登録済み版の不正変更防止オーバーレイ40'が検出されロードされ、独自の暗号キー-20'を使用することにより、登録済み版のエグゼクティブブリューループが解読され実行される。このようにして、デモンストレーション版は完全に動作する登録版に変換される。

プログラムの操作向上版が利用できる場合、使用者は同一のプロセスを実行してさらに別の解説キーと、より強化されたニゲゼタディアブリューループと追加プログラムファイルを有する別の不正変更防止オーバーレイとを受信して、より強化された版の製品に更新することができる。

様々な実施例が、小さな不正変更防止オーバーレイを使用して大きなプログラムの制御を行なうための追加的機能を提供す

特許平6-501120(7)

用することができる。このような枚挙は、ここにも含まれているようだ。プログラムの部分あるいはプログラムを転送用指定期と結合する形式で記述するための、ここに開示されている方法がもたらす両面的利益の可能性の早くなる例である。

上記の知見に照らし合わせ、本発明に最も近い実用例が可能なことは明らかである。たとえば、本発明は、使用者のコンピュータがその地域の登録用コンピュータに接続され、さらにその登録用コンピュータがそれより広い地域の登録用コンピュータに接続され、というように移動構造的に実装することも可能である。その場合は登録用コンピュータの登録権限は、その地域の登録用コンピュータとそれより広い地域の登録用コンピュータとの契約に含まれる使用許諾契約によって制御できるであろう。したがって、下記の審査請求の範囲であれば、本発明を上記実用例に開示されている以外の方法で実施することができる。

図2

立候過程

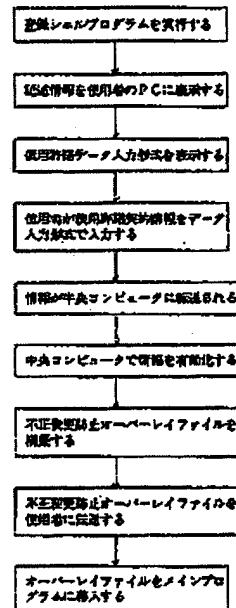
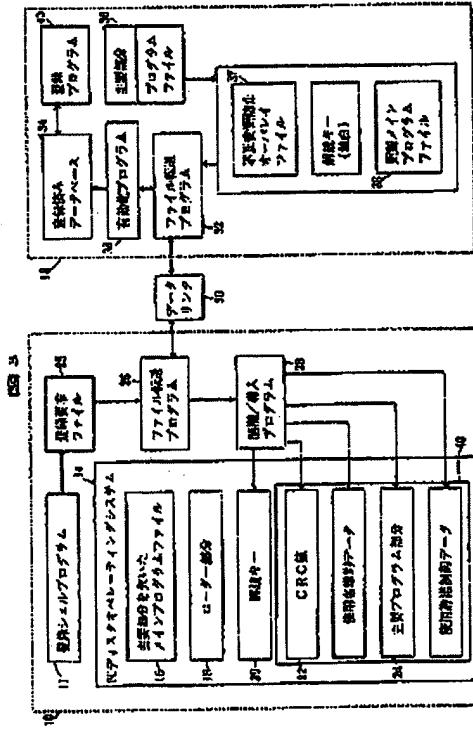
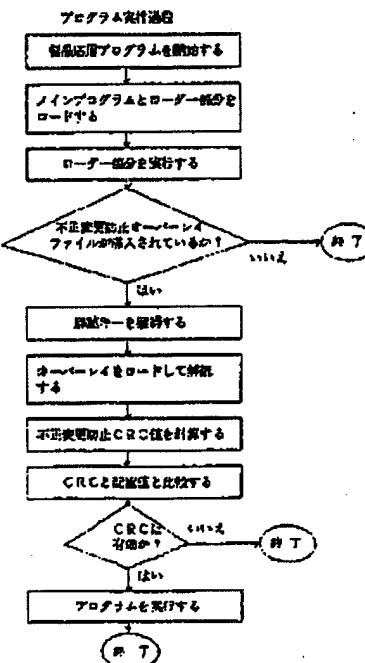
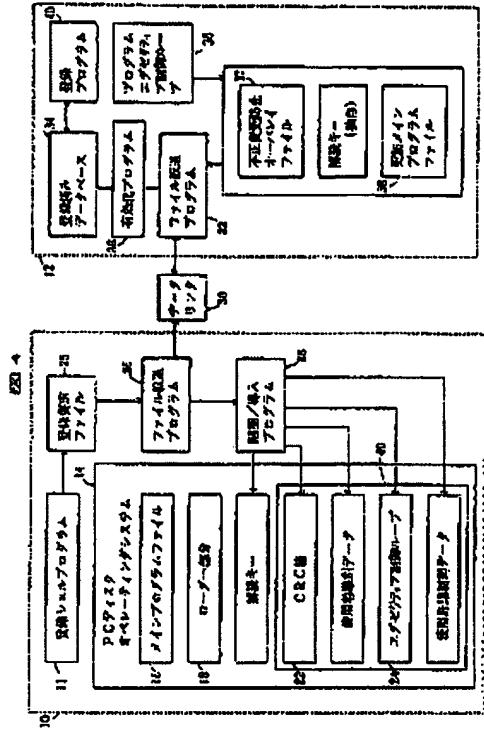


図2



特頁平6-501120 (8)

◎ 球形素描



フロントページの锯き

(51) Int.Cl.⁵ 諸別記号 廣内整理番号 F 1
H 04 L 9/12

(61)指定期 E.P.(AT. BE. CH. DE.
DK. ES. FR. GB. GR. IT. LU. NL. S
E), CA. JP